Chapter 1 Answers to Review Questions and Exercises

Review Questions

1. What is the difference between a threat agent and a threat?

A threat agent is the facilitator of an attack, whereas a threat is a category of objects, people, or other entities that represents a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences and others are purposeful. Fire is a threat; however, a fire that has begun in a building is an attack. If an arsonist set the fire, then the arsonist is the threat agent. If an accidental electrical short started the fire, the short is the threat agent.

2. What is the difference between vulnerability and exposure?

Vulnerability is a weakness or fault in a system or protection mechanism that opens it to attack or damage. Exposure is a condition or state of being exposed. In information security, exposure exists when a vulnerability is known to an attacker.

3. How is infrastructure protection (assuring the security of utility services) related to information security?

The availability of information assets is dependent on having information systems that are reliable and that remain highly available.

4. What type of security was dominant in the early years of computing?

In the early years of computing, if security was addressed at all, it dealt only with the physical security of the computers themselves and not the data or connections between the computers. Consequently, most information stored on computers was vulnerable because information security was left out of the design phase of most systems.

5. What are the three components of the C.I.A. triad? What are they used for?

The three components of the C.I.A. triad are:

 Confidentiality (assurance that information is shared only among authorized people or organizations)

 Integrity (assurance that the information is complete and uncorrupted)

 Availability (assurance that information systems and the necessary data are available for use when needed)

These three components are frequently used to conveniently articulate the objectives of a security program that must be used in harmony to make sure an information system is secure and usable.

6. If the C.I.A. triad is incomplete, why is it so commonly used in security?

The C.I.A. triad is commonly used in security because it addresses the fundamental concerns of information: confidentiality, integrity, and availability. It is used despite being incomplete because it addresses all major concerns with the vulnerability of information systems.

7. Describe the critical characteristics of information. How are they used in the study of computer security?

The critical characteristics of information define its value. Changing any of its characteristics changes the value of the information itself. There are seven characteristics of information:

 Availability enables authorized users—either people or computer systems—to access information without interference or obstruction, and to receive it in the required format.

 Accuracy occurs when information is free from mistakes or errors and has the value that the end user expects.

 Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

 Confidentiality is achieved when disclosure or exposure of information is restricted only to authorized individuals or systems. Confidentiality ensures that only people with the rights and privileges to access information are able to do so.

 Integrity of information is maintained when it is whole, complete, and uncorrupted.

 Utility of information is the quality or state of the information having value for some particular purpose or end.

 Possession of information is the quality or state of ownership or control of some object or item. Information is said to be in one’s possession if one obtains it, independent of format or other characteristics.

8. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?

The six components are software, hardware, data, people, procedures, and networks.

People would be affected most by the study of computer security. People can be the weakest link in an organization’s information security program. Unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate people to obtain access information about a system.

Procedures, written instructions for accomplishing a specific task, could be another affected component. The information system will be effectively secured if employees are taught to follow and safeguard procedures. Following procedure reduces the likelihood of employees erroneously creating information insecurities. Proper education about the protection of procedures can avoid unauthorized access through social engineering. Hardware and software are the components that are historically associated with the study of computer security. However, networking is the component that created much of the need for increased computer and information security.

9. What system is the predecessor of almost all modern multiuser systems?

MULTICS is the predecessor of almost all modern multiuser systems.

10. Which paper is the foundation of all subsequent studies of computer security?

RAND Report R-609, sponsored by the Department of Defense paper, is the foundation of all subsequent studies of computer security.

11. Why is the top-down approach to information security superior to the bottom-up approach?

The top-down approach, in which a project is initiated by upper-level managers who issue policy, procedures, and processes; dictate the goals and expected outcomes; and determine accountability for each required action; has a higher probability of success. This approach has strong upper management support, a dedicated champion, usually dedicated funding, a clear planning and implementation process, and the means of influencing organizational culture. The most successful kind of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

12. Why is a methodology important in the implementation of information security? How does a methodology improve the process?

A methodology is a formal technique that has a structured sequence of procedures used to solve a problem. Methodology is important in the implementation of information security because it ensures that development is structured in an orderly, comprehensive fashion. The methodology unifies the process of identifying specific threats and the creation of specific controls to counter those threats into a coherent program. Thus, a methodology is important in the implementation of information security for several reasons:

 First, it entails all the rigorous steps for an organization’s employees to follow, which helps them avoid unnecessary mistakes that may compromise the goal of having a comprehensive security posture. A methodology guides an organization to solve the root cause of the information security problem, not just its symptoms.

 Second, a methodology increases the probability of success. Once a methodology is adopted, selected personnel will be responsible for establishing key milestones and made accountable for achieving the project goals.

 The methodology can greatly improve the process. For example, following the six steps of the systems development life cycle (investigation, analysis, logical design, physical design, implementation, and maintenance and change) allows development to proceed in an orderly, comprehensive fashion. Individuals or groups assigned to the analysis step do not have to begin work until the investigation step is finished. Moreover, each step of the methodology may determine whether the project should be continued, discontinued, outsourced, or postponed. For example, the physical design step may need to be postponed or outsourced if the organization does not possess the technology needed.

13. Which members of an organization are involved in the security systems development life cycle? Who leads the process?

Initiation and control of the SecSDLC is the responsibility of upper management. Responsible managers, contractors, and employees then execute the SecSDLC. The process is usually led by a senior executive, sometimes called the *champion*, who promotes the project and secures its financial, administrative, and company-wide backing. A project manager is assigned the task of managing the project.

14. How can the practice of information security be described as both an art and a science? How does the view of security as a social science influence its practice?

The practice of information security is a never-ending process. An effective information security practice must be considered as a tripod that relates to three important aspects (science, art, and social science):

First, information security is a science because it requires various kinds of tools and technologies used for technical purposes. It can also include sound information security plans and policies that may dictate the needs of particular technologies.

Second, information security is also an art because there are no clear-cut rules for how to install various security mechanisms. Different factors such as budgets, time, threats, risks, vulnerabilities, and asset values can significantly affect the numbers and types of passive and active controls an organization needs. The overall goal is for the organization to have a sound information security posture that can reduce the risks of being attacked as much as possible.

Third, and most importantly, information security must be examined as a social science because social science deals with people, and information security is primarily about people, not technology. Through the eye of a social scientist, an organization can greatly benefit from the Security Education, Training, and Awareness program (SETA), which can help employees understand how to perform their jobs more securely, be fully aware of the security issues within the organization, and be accountable for their actions.

Therefore, information security must be viewed from all three standpoints, with the most emphasis on the social science perspective. After all, people create the other five components of information assets (software, hardware, data, procedures, and networks).

15. Who is ultimately responsible for the security of information in the organization?

The chief information security officer (CISO) is primarily responsible for the assessment, management, and implementation of information security in the organization. The CISO usually reports directly to the CIO, although in larger organizations, one or more layers of management might exist between the two. However, the recommendations of the CISO to the CIO must be given equal if not greater priority than other technology and information-related proposals.

16. What is the relationship between the MULTICS project and the early development of computer security?

MULTICS, or Multiplexed Information and Computing Service, was the first operating system created with security as its primary goal. It was a mainframe, time-sharing operating system developed through a partnership among GE, Bell Labs, and MIT. Much of the early focus for research on computer security was centered on this system.

17. How has computer security evolved into modern information security?

Before the creation and use of networking technologies, computer security consisted of securing a system’s physical location with badges, keys, and facial recognition. With the creation of ARPANET and the increasing popularity of networked systems, it was no longer adequate just to physically secure a system. To ensure total security, the information itself, as well as the hardware used to transmit and store it, needed to be protected. Information security developed from this need. Eventually, computer security became just another component of information security.

18. What was important about RAND Report R-609?

The movement toward security that went beyond protecting physical locations began with RAND Report R-609, a paper sponsored by the Department of Defense. This report attempted to address the multiple controls and mechanisms necessary for the protection of a multilevel computer system. In addition, the RAND Report was the first to identify the role of management and policy issues in the expanding arena of computer security. It noted that the wide use of networking components in military information systems introduced security risks that could not be mitigated by the routine practices used to secure these systems. This paper signaled a pivotal moment in the history of computer security—the scope of computer security expanded significantly from the safety of physical locations and hardware to include securing data, limiting random and unauthorized access to it, and involving personnel from multiple levels of the organization in information security.

19. Who decides how and when data in an organization will be used or controlled? Who is responsible for seeing that these decisions are carried out?

The three types of data ownership and their respective responsibilities are:

 Data owners, who are responsible for the security and use of a particular set of information. They are usually members of senior management and could be CIOs. The data owners usually determine the level of classification associated with the data, as well as changes to that classification required by organizational change. Data owners work with subordinate managers to oversee the day-to-day administration of the data.

 Data custodians, who work directly with data owners and are responsible for the storage, maintenance, and protection of information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

 Data users are end users who work with the information to perform their daily jobs and support the mission of the organization. Everyone in the organization is responsible for data security, so data users are included here as individuals with an information security role.

20. Who should lead a security team? Should the approach to security be more managerial or technical?

A project manager, who may be a departmental line manager or staff unit manager, would lead a security team. Typically, that person would understand project management, personnel management, and the technical requirements of information security. The approach to security should be more managerial than technical, although the technical ability of the resources who perform day-to-day activities is critical. The top-down approach to security implementation is by far the best. It has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the opportunity to influence organizational culture.

Exercises

1. Look up “the paper that started the study of computer security.” Prepare a summary of the key points. What in this paper specifically addresses security in previously unexamined areas?

RAND Report R-609 noted that security for computers had moved beyond the physical security of locking them behind closed doors. With the rise in computer networking, multiple users of resource-sharing systems could gain access to confidential information. New forms of security had to be implemented to protect the safety of data, limit access, and handle different levels of personnel accessing the system. R-609 pointed out that a task force was being implemented by ARPA to focus on the potential security risks of multi-access computer systems. The paper stated that security was no longer as simple as moving the system to a secure location, and that new measures must be implemented to provide acceptable security.

The key points of the paper addressed security control in resource-sharing systems; the increased number of resource-sharing systems; protection of information in multi-access, resource-sharing computer systems; and the needed application of security rules and regulations.

The growing need to make resources available to a larger number of users led to the implementation of resource-sharing computer systems in the 1960s. Sharing data among more users highlighted the need for an appropriate security system because data in a multi-access computer environment was no longer considered secure. Above all, the lack of control demonstrated by random and unauthorized access to shared data started to be seen as one of the biggest threats to the data itself. Another important issue was the lack of security rules and regulations. RAND Report R-609 was the first report to identify the important role of management and policy issues in computer security.

2. Assume that a security model is needed for the protection of information in your class. Using the CNSS model, examine each of the cells and write a brief statement on how you would address the three components of each cell.

Confidentiality – Policy – Storage: An example of protecting the confidentiality of class information in storage by means of policy would be issuing rules to keep access restricted to unauthorized viewers. One such rule could be to lock file cabinets that contain the information.

Confidentiality – Policy – Processing: An example of protecting the confidentiality of class information in processing by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being processed. For instance, only registered students in the class should be allowed to attend and listen to lectures.

Confidentiality – Policy – Transmission: An example of protecting the confidentiality of class information in transmission by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being transmitted. For instance, a policy may require that all transmission of confidential data over public networks must be encrypted.

Confidentiality – Education – Storage: An example of protecting the confidentiality of class information in storage by means of education would be to train students and faculty about which people have authorized access to the information in storage.

Confidentiality – Education – Processing: An example of protecting the confidentiality of class information being processed by means of education would be to train students and faculty to verify whether people are authorized to get the information before class starts by using a student ID or schedule.

Confidentiality – Education – Transmission: An example of protecting the confidentiality of class information being transmitted by means of education would be to train students and faculty to close classroom doors during a lecture so that others outside could not hear it.

Confidentiality – Technology – Storage: An example of protecting the confidentiality of class information being stored by means of technology would be using locks on file cabinets that contain the information while not in use.

Confidentiality – Technology – Processing: An example of protecting the confidentiality of class information being processed by means of technology would be forcing the use of electronic IDs during classes.

Confidentiality – Technology – Transmission: An example of protecting the confidentiality of class information being transmitted by means of technology would be having a password on a class Web site.

Integrity – Policy – Storage: An example of protecting the integrity of class information being stored by means of policy would be a simple rule that only certified people may alter the information.

Integrity – Policy – Processing: An example of protecting the integrity of class information being processed by means of policy would be a rule that forces students to study in quiet areas without the help of people who are not in the class.

Integrity – Policy – Transmission: An example of protecting the integrity of class information being transmitted by means of policy would be a rule that the teacher is not allowed to drink alcohol before class.

Integrity – Education – Storage: An example of protecting the integrity of class information being stored by means of education would be teaching people who store the information the names and roles of others who are authorized to change it.

Integrity – Education – Processing: An example of protecting the integrity of class information being processed by means of education would be informing students not to risk receiving incorrect information by studying with people who are not in the class.

Integrity – Education – Transmission: An example of protecting the integrity of class information being transmitted by means of education would be providing instructors with effective ways to teach.

Integrity – Technology – Storage: An example of protecting the integrity of class information being stored by means of technology would be electronically storing all data on a device that requires authorization to modify.

Integrity – Technology – Processing: An example of protecting the integrity of class information being processed by means of technology would be creating PowerPoint presentations to verify what the teacher says.

Integrity – Technology – Transmission: An example of protecting the integrity of class information being transmitted by means of technology would be printing the PowerPoint presentations and giving a copy to each student.

Availability – Policy – Storage: An example of protecting the availability of class information being stored by means of policy would be a policy that only authorized students are allowed access to certain stored information.

Availability – Policy – Processing: An example of protecting the availability of class information being processed by means of policy would be a rule that only authorized people are allowed to enter the classroom.

Availability – Policy – Transmission: An example of protecting the availability of class information being transmitted by means of policy would be a rule that only students are allowed into the classroom.

Availability – Education – Storage: An example of protecting the availability of class information being stored by means of education would be teaching correct storage processes so information doesn’t get lost.

Availability – Education – Processing: An example of protecting the availability of class information being processed by means of education would be instructing those who teach the information to speak up so everyone in the classroom can hear.

Availability – Education – Transmission: An example of protecting the availability of class information being transmitted by means of education would be teaching students to remain quiet in the classroom so everyone can hear.

Availability – Technology – Storage: An example of protecting the availability of class information being stored by means of technology would be making the information available on the Internet via a password-protected Web site.

Availability – Technology – Processing: An example of protecting the availability of class information being processed by means of technology would be a teacher making PowerPoint files available to students via the Internet.

Availability – Technology – Transmission: An example of protecting the availability of class information being transmitted by means of technology would be a teacher using a microphone so lectures are loud enough for all students to hear.

3. Using the Web, identify the chief information officer (CIO), chief information security officer (CISO), and systems administrator for your school. Which of these people represents the data owner? Which represents the data custodian?

Each organization has its own answers depending on its policies.

4. Using the Web, find a large company or government agency that is familiar to you or located in your area. Try to find the name of the chief executive officer (CEO), the CIO, and the CISO. Which was easiest to find? Which was hardest?

While each organization has its own answers depending on its policies, a recent trend is that organizations protect the personal identity of some security-related staff.

5. Using the Web, find out more about Kevin Mitnick. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.

Kevin Mitnick was one of the most notorious hackers in computer history. He began his hacking career by using a personal computer and a modem to gain access to a digital central office switch of a local telephone company. He and several other members of a phone phreak gang would make prank calls, answer operator-assisted calls, and eavesdrop on conversations. However, these activities didn’t satisfy them for long. In 1981, over Memorial Day weekend, Mitnick and his gang talked their way past a security guard at Pacific Bell’s COSMOS center. Once inside, they stole passwords, operating manuals, and combinations to doors at other Pacific Bell offices. They also performed some “social engineering” while inside and left fake names and phone numbers for later use. The gang was eventually caught when a girlfriend of one of the members went to the police. The gang was charged with stealing and destroying data. Mitnick was only 17 at the time, and was sentenced to three months in juvenile detention and one year of probation. In 1983, Mitnick was arrested again, this time by the campus police at the University of Southern California. He had used one of the school’s computers to break into the Pentagon using ARPANET. His sentence was six months in a juvenile prison. In 1987, he received three years probation for stealing software from the Santa Cruz Operation. He was caught through his use of illegal telephone credit card numbers.

In 1989, he was again arrested and charged with one count of possession of illegal long-distance access codes and one count of computer fraud. He and a friend tried to gain access to Digital Equipment’s Palo Alto research laboratory with the hope of acquiring a copy of the VMS minicomputer operating system. He was caught when his accomplice became frustrated with him and turned him in to the FBI and DEC. Mitnick received jail time and was required to undergo counseling at a halfway house. In 1992, an arrest warrant was issued when he violated the terms of his probation by associating with members of his original phone phreak gang and illegally accessing a computer. Mitnick was arrested in 1995.

Alternate Answer

Kevin Mitnick, a.k.a. Condor, is one of the most famous hackers in the history of computers. He was so prolific that he earned a place on the FBI’s Most Wanted List. Mitnick started as a phone phreaker, someone who breaks into phone switches, but later he turned his attention to computer systems. Mitnick was brought up on charges numerous times, but he made national attention with a computer hacking spree in 1995. Mitnick was finally tracked down after two years on the run as a fugitive. Tsutomu Shimomura played a major role in the capture after his computer system was hacked by Mitnick. Mitnick was jailed for five years without a trial or bond, and is said to be the longest-held American prisoner without a trial. Mitnick was released in 2000, but was prohibited from using any electronic device as a term of his probation.

6. Using the Web, explore the technique known as “iterative and incremental development.” Then, investigate “agile development.” How are they related?

Agile is a later manifestation of the core principles of iterative and incremental development. So-called lightweight agile software development methods arose in the 1990s in response to cumbersome waterfall-oriented methods. Waterfall development had emerged as a more widely adopted methodology than iterative and incremental development. Supporters of agile methods argue that they achieve better results by being more responsive to user needs.